Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 79 (2016) 410 – 418
Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Signature Verification SaaS Implementation on Microsoft Azure Cloud

Joel Philip[a], Dr. Vinayak A Bharadi[b]

[a]*M.E Student, Department of Information Technology, Thakur College of Engg. and Tech., Mumbai -400101, India*
[,b]*Associate Prof., Department of Information Technology, Thakur College of Engg. and Tech., Mumbai -400101, India*

Abstract

Signature recognition is one of the important behavioral biometric trait. Signatures recognition systems can be used to identify precisely user identity by making use of signature information such as x, y variations and pressure from a tablet PC. This makes way for using dynamic, i.e., online handwritten signature based biometric system is more accurate than the static ones, hence can be useful for signature verification applications. In this paper new set of features are proposed for online or dynamic signature recognition. In this research, feature vector and their extraction mechanism is implemented using Webber Local Descriptor (WLD). Thus, helping signature verification applications to detect forgery of signatures. The performance of proposed feature vector is further improved by soft biometric traits of the signature.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Biometrics, Banking Applications, Webber Local Descriptors, Texture Features, Online Dynamic Signature, Pressure, Windows Tablet PC, Azure, Cloud Services, Cloud Computing, REST API, K-nearest neighbourhood, Classification.

1. Introduction

With the sudden technology-outburst in the recent past, security is one of the biggest rising concern in the real world as well as online systems. Human identification and authentication is an important criterion for the surveillance systems in real world as well as online security systems. Biometrics is the most efficient answer for all the problems and it has been widely accepted.

A. Biometrics

Biometric authentication has grown in popularity as a way to provide personal validation. The identification of a human can be defined by the uniqueness of the person; to measure the uniqueness and a person's behavioral characteristics, biometric can be used. The different biometric features of the human body includes the eyes, fingerprint, human face, signature, palm, retina, and iris. A person's identification is critically significant in many

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.053

applications and the rapid rise in credit card fraud and identity theft in recent years indicate that this is an issue of major concern in wider society. Individual passwords, pin identification or even token based arrangement all have limitations which restrict their applicability in a widely-networked society. Biometric is used to identify the identity of an input sample when compared to a predefined template, used in cases to validate and identify specific people by certain characteristics. Biometric systems are able to provide efficient and secured way of authentication to users. When we compare this system with the traditional authentication systems which are based on token or password, it is definite that biometric system is more safe, efficient and robust. This is because, token and password are known to the users or in the possession users, which can be forgotten or stolen.

These security concerns does not affect in biometric system, which is an alternative method for person identification and verification. In the identification mode person's identity can be extracted from the database where in case of verification mode person's identity can be authenticated on basis of his/her claim. Physiological and behavioral features can be defined as the types of biometrics.

Physiological features are measurement of biological traits of users, like fingerprint, retina, iris and face. The behavioral traits of users can be enlisted as signature and voice. To process such traits recognition system will be called as biometric system.

B. Processing Steps

Signatures are classified into two categories offline (or static) and online (or dynamic) signature on the basis of signature acquisition and recognition method. Online signature verification uses the dynamic characteristics of the signature to authenticate the user. Learning dynamic signature is very difficult task and to replicate as well. The processing steps involves the use of active stylus as input on devices such as Personal Digital Assistants, tablet PC's and smart phone, contributes to the basic pre-requisites of capturing or acquiring dynamic signature. The initial step involved in dynamic signature is primarily to capture user signature from a Windows tablet PC interface. This acquisition includes capturing the signature along with each strokes of signature with its X, Y coordinates and pressure sensitivity being stored as packets of information. This is followed by processing it further by performing feature extraction and finally classification of the same.

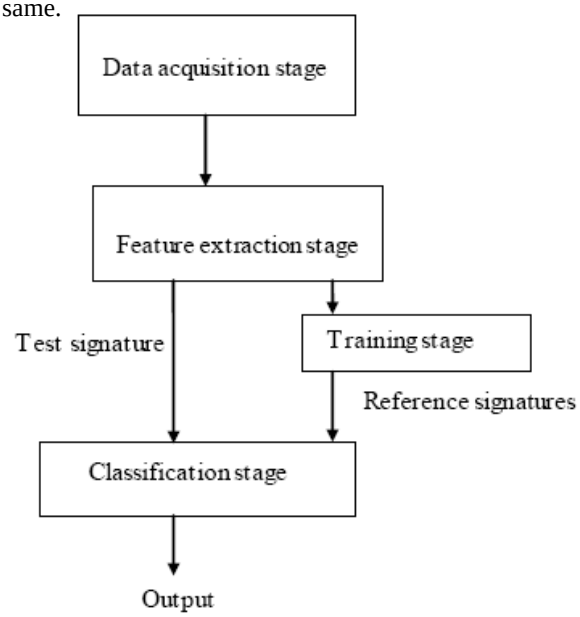

Figure 1.1 Processing Steps of Signature

C. Biometric SaaS Banking Application

As emphasized, there are certain aspects of biometric systems for banking applications, which heavily rely on cloud computing. Primarily, the biometric computation logic is located in the cloud and not on a local processing unit, as it is the case with existing biometric recognition systems. This characteristic makes the cloud based biometric technology globally accessible and provides the necessary means for integration in other security and/or consumer

applications. This is further enhanced by the use of REST API instead of SOAP API, which will enable thin client framework to easily access the proposed architecture, without the user being burdened with complex computational workload. Second of all, storing biometric data in the cloud makes the system highly scalable and allows quick and reliable adaptation of the technology to an increasing user base, who may be mobile or desktop consumers. On the other hand, storing biometric data in the cloud may raise privacy concerns and may not be in accordance with national legislation. Last but not least, a cloud implementation of biometric technology may harvest all merits of the cloud, such as real-time and parallel processing capabilities, billing by usage etc. All of the presented characteristics make cloud-based biometric recognition technology extremely appealing. In [1] Abdullah A. Albahdal and Terrance E. Boult, have stated that biometric authentication can be a solution for most of the authentication problems. Where password-based authentication authenticates users based on something the user knows, biometric authentication authenticates users based on "something they are". In other words, biometrics authentication identifies users based on their biological or behavioral characteristics. Hence, biometrics are superior to password-based authentication because biometrics provide stronger authentication, are more usable (user does not require to remember a lot of long and complex passwords), and biometrics cannot be easily stolen, forgotten, or guessed.

2. Literature Survey

One of the main aims of this research is to empower biometrics as an authentication method for security purposes like accessing a particular service or bank applications etc. But the first question to be addressed is: why enable biometrics for authentication?

The security and usability problems [1] of password-based authentication, which is the most commonly used authentication method for secure access, have been reviewed. Many theoretical studies in the literatures show that password-based authentication suffers from a wide-range of attacks including brute force, dictionary, sniffing, shoulder surfing, phishing, and key-logger attacks. In addition, human elements add additional security weaknesses to the password-based authentication. For example, users are likely to write down their passwords, use the same password across-multiple systems, use the same password over a long period of time, and share their passwords with their co-workers, family members, or friends. Sasse et al. [2] experimentally investigate the main causes of password problems such as memorability issues and technical/organizational requirements (e.g., forced change of password). This study concludes that Human Computer Interaction (HCI) techniques can be used to address password problems. Similarly, Yan et al. [3] empirically study passwords memorability and securityAn array of researches have been made in the biometric field of stroke based signature recognition. Some methods used are implemented using a digitizer, which needs to be explicitly used for the sole purpose of capturing signatures.

Existing methods for implementing signature recognition on digitizer device are effective. In [4] modified digital difference analyzer algorithm is proposed which captures dynamic characteristics of signature in discrete values. In [5] the authors have explained time based vector quantization by Kekre's Median Codebook Generation Algorithm which gives information about the nature of signature and pressure applied while signing. In [6] image and texture analysis of dynamic signatures have been proposed using Gabor Filters. In another implementation [7] dynamic features of signature such as spatial co-ordinates, pressure, azimuth, altitude variation is analysed and then extracted using transforms such as DCT, FFT, WHT and Kekre's Transforms.

In [8] authors describe how computationally intensive biometric recognition can be performed on a mobile device by offloading the actual recognition process to the cloud. The authors have proposed a systematic approach for dividing a recognition operation and a bulk enrollment operation into multiple tasks, which can be executed in parallel on a set of servers in the cloud, and shown how the results of each task can be combined and post-processed for individual recognition.

In [9] authors have proposed a off-line signature recognition & verification using back propagation neural network, where the signature is captured and presented to the user in an image format. Signatures are verified based on features extracted from the signature using Invariant Central Moment and Modified Zernike Moment for its invariant feature extraction.

In [10] a framework of off-line signature recognition & verification using neural-fuzzy is proposed, where the signature is catch and presented to the user in an image format. Signatures are verified depend on parameters extracted from the signature using various image processing techniques. Then Off-line Signature Recognition and Verification is implemented with SURF features and Neural Fuzzy techniques in ANFIS in Matlab.

All these methods have been implemented only on digitizer tablets but have not yet been implemented on any Windows Tablet-PC.

3. Problem Statement

Signatures are also the behavioural describing characteristics of a humans. The methods for writing a signature differs from person to person, which includes the curve, stroke, lines and dot as well. At the initial stage the signature will be accepted as input on a Microsoft Tablet PC [Dell Venue Pro Tablet] and then it will be processed further, such methods can be called as online signature recognition. After capturing the signature it's given to the Web role in the cloud service which uploads the file in the blob storage in cloud. Then in the Worker role of the cloud service, cluster-based feature vector is applied on the uploaded signature in the blob storage to generate the feature vector of the signature and vectorization will be performed, further the feature vector can be tested and compared with the set of blob storage. At the last stage results will be computed and notified to the client.

- To make research on the signatures and design an interface to capture the signature on Windows tablet [Dell Venue Pro 8].
- Collect information of signatures' X, Y coordinates and stylus pressure while signing it on the interface using Active Stylus [Dell Active Stylus].
- Authenticate the client using OAuth 2 authorization framework
- Upload the signatures in the BLOB storage using a Web Role in the Cloud.
- Compute the feature vector of signature using a Worker Role in the cloud and store it in the BLOB storage, thereby implementing Vector Quantization generating vectors using Kekre's Fast Code Book Generation or any other such feature.
- Perform verification of signature using a Web Role and Worker Role and notify the client with the appropriate result.
- Devise highly Scalable, Pluggable and Faster online signature recognition system as a SaaS Model.

4. Proposed Idea

Internet banking, networking, e-Government and other new technologies have seen an ever increasing use in the last years. Ensuring security is the most vital problem in these environments. Biometric-based solutions to this problem are currently the most sought after topic. Biometrics are widely used and measured as important system in terms of security of banking applications. Human signatures are one of those important traits, used for personal identification. Generally, signature recognition [11] systems need to be executed on a high ended machine, like digitizer, to perform operations of enrolment and verification of signatures. But when multiple enrolment and verification tasks are to be performed the performance degrades. And it's also prone to single point of failure. Moreover over the past years the amount of online signature biometric data that need to be stored is increasing at a very faster rate.

This research aims to satisfy such expectations by creating a dynamic online signature framework technology on Tablet PC computed to a cloud platform which will devise a highly Scalable, Pluggable and Faster online signature recognition system, capable of operating on enormous amounts of data, which, in turn, induces the need for sufficient storage capacity and significant processing power, for online banking applications which implements signature recognition.

Users using the banking application need to be enrolled by capturing their signatures, this will be done by a Windows Tablet PC which will accept the input as a signature using Active Stylus. This signatures are uploaded to the blob storage using the web role in the cloud. After storing the signatures, the web role posts a work item to a queue for feature extraction. The worker role fetches the work item from the queue, retrieves the signatures from blob storage, and extract the feature vectors. This extracted feature vectors is then stored in blob storage. There will be a web role and worker role to identify the user's signature from the set of records in blob storage.

The signature recognition systems, that exist in the market needs high ended machine like digitizer, to perform operations of enrolment and verification of signatures. Yet, it results in low performance when required to do multiple enrolment and verification of signatures and it also depends on feature vector extraction mechanism, to add to it, even single point of failure may occur. Moreover over the past years the amount of online signature biometric data that need to be stored is increasing at a very fast rate. Such expectations make it necessary to devise highly Scalable,

Pluggable and Faster online signature recognition system, capable of operating on enormous amounts of data, which, in turn, induces the need for sufficient storage capacity and significant processing power.

To overcome foresaid need, this research has selected cloud computing to resolve the outlined issues, by moving the existing biometric technology to a cloud platform that ensures appropriate scalability of the technology, sufficient amounts of storage, parallel processing capabilities and with the widespread availability of mobile tablet PC devices provides an accessible entry point for various applications and services that rely on mobile clients. Hence, cloud computing is capable of addressing issues related to the next generation banking applications based on biometric technology

The basic system need to do following operation:

1. Enrol signature samples from users through a dynamic interface on Windows Tablet which recognizes user input from Active Stylus storing its X, Y coordinates and pressure information as input values.
2. Verify the stored signature using Azure cloud services and feature extraction method of Webber Local Descriptor.

5. Background of Technologies Used

The proposed methodology implements Webber Local Descriptor for feature extraction of signature which has been captured:

A. Webber Local Descriptor (WLD)

It is a psychological law. It states that the change of a stimulus (such as lighting, sound) that we just notice is a constant ratio of the original stimulus. A human being would recognize it as background noise rather than a valid signal, when the change is smaller than this constant ratio of the original stimulus. The differential excitation component of the proposed Weber Local Descriptor (WLD) is computed for a given pixel. It is the ratio between the two terms: first is the intensity of the current pixel; the second is the relative intensity differences of a current pixel against its neighbours (e.g., 3 X3) square regions. We attempt to extract the local salient patterns in the input image, with the differential excitation component. In addition to this, current pixel's gradient orientation is also computed. For each pixel of the input image, we compute two components of the WLD feature which are differential excitation and gradient orientation. We represent an input image (or image region) with a histogram by combining the WLD feature per pixel. We call a WLD histogram hereinafter. Hence we call WLD a dense descriptor. The proposed WLD descriptor employs the advantages of SIFT using the gradient and its orientation in computing the histogram, smaller support region and those of LBP in computational efficiency. But WLD differs from Local Binary Pattern and SIFT. As WLD is a dense descriptor, computed for every pixel and depends on the magnitude of the centre pixel's intensity and both the Texture classification local intensity variation and with WLD is carried out using 2D WLD histograms. [12]

Texture classification local intensity variation and with WLD is carried out using 2D WLD histograms. A short literature review reveals that recent trends in feature selection for offline signature verification are based on grey level information and supplementary texture grey level information [13]. A different approach considers curvature of the most important segments and introduces a graph metric feature set. Another interesting issue is that feature used in the analysis of writer verification and identification tasks could be employed in order to examine the signature image as a textural signal. Then, textural features could be used in order to represent the feature space.

Signature verification cannot be done by character recognition alone because the alphabets of signature cannot be read out separately and it appears as an image with some curves representing the writing style of an individual. So, a signature image can be considered as a special distribution of pixels representing writing style rather than a collection of alphabets, hence, WLD method is adopted in this research.

B. Microsoft Azure Cloud Services

When creating an application and running it in Azure, the code and configuration together are called an Azure cloud service. By creating a cloud service, one can deploy a multi-tier web application in Azure, defining multiple roles to distribute processing and allow flexible scaling of your application. A cloud service consists of one or more web roles and/or worker roles, each with its own application files and configuration. "Web Role" virtual machines are Windows Servers with IIS installed, whereas "Worker Role" virtual machines are Windows Servers without IIS installed. The greatest thing about Web Roles is that it don't need to maintain the operating systems or virtual machines. Azure guarantees that the VMs are up to date, and will automatically replace them with fresh versions if

they fail. A cloud service often consists of one or more web roles and/or worker roles, each with its own application files and configuration.

C. Microsoft Visual Studio .NET 2015

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web applications and web services. The Microsoft.Ink API required for interfacing Windows tablet PC. This is used along with Microsoft Azure services in MS Visual studio .NET for implementing the proposed cloud based biometric solution.

6. Proposed Methodology

- Enrolment:

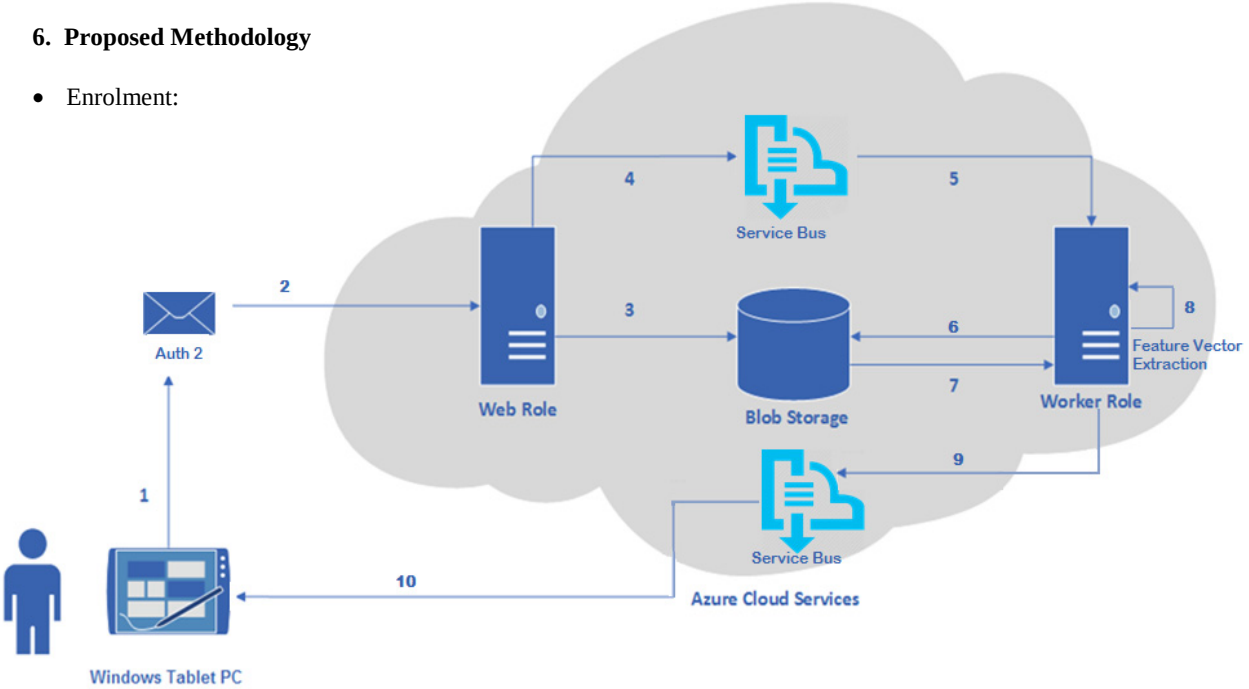

Figure 1.2 Enrolment Operation Architecture on Azure Cloud

Take signature samples from users through a dynamic interface on Windows Tablet which recognizes user input from Active Stylus storing its X, Y coordinates and pressure information as input values. Enrolment operation consists of capturing the signatures from the Windows Tablet PC, authenticating the user using OAuth2 authorization and uploading this signature in the blob storage in the cloud using a web role. It also consists of background processing of feature extraction done by the worker role on the uploaded signatures. After feature extraction, storing this feature vector of the signature in the blob storage is done. The enrolment operation step by step execution is shown in Fig 1.2

- Verification:

Verification operation consist of verifying whether the signature is valid one or not. There are various methods in current market for verifying signatures using methods such as neural network [14], back propagation [8], dominant point feature [15] etc. Calculating the feature vector of the verifying signature and comparing this calculated feature vector with the feature vectors stored in the blob storage. If the calculated feature vector matches with the feature vector in the blob storage then it's a valid signature or else it's an invalid signature. Feature extraction is done using Webber Local Descriptor.

The verification operation consist of similar steps as the enrolment operation steps but it also consist of some more steps for verification of the signature. In the verification operation, first capture the signature from the Windows Tablet PC and upload the signature to be verified to the web role, along with the stroke information. The web role will store this signature temporary with a different container name in the blob storage. After storing the signature, the web role posts a work items to a queue to have the Feature vector calculated for the uploaded signature and checks whether the

signature is valid or invalid. The worker role here will perform two tasks first is to calculate the feature vector of the verified signature and second is to perform verification operation by checking whether there is any match between the calculated feature vector and stored feature vectors in the blob storage.

The worker role pass the appropriate result to the web role, which will first send the response to the client and then delete the verification signature template from the blob storage. The verification operation steps by step execution is shown in Figure 1.3

- Feature Selection

The feature selection (or dimensionality reduction) module is employed as not all the detected features are useful. Here, only a subset of representative features are used to extract the features of the signature. Doing feature selection gives us the relevant features and thus the more accurate and precise result. It also gives us an additional advantage of faster computation time as the dimensionality of data is reduced. In this research, the feature selection technique employed is Webber Local Descriptor. WLD consists of two components: its differential excitation and orientation. A differential excitation is a function of the ratio between two terms: One is the relative intensity differences of its neighbors against a current pixel; the other is the intensity of the current pixel. An orientation is the gradient orientation of the current pixel. For a given image, we use the differential excitation and the orientation components to construct a concatenated WLD histogram feature.

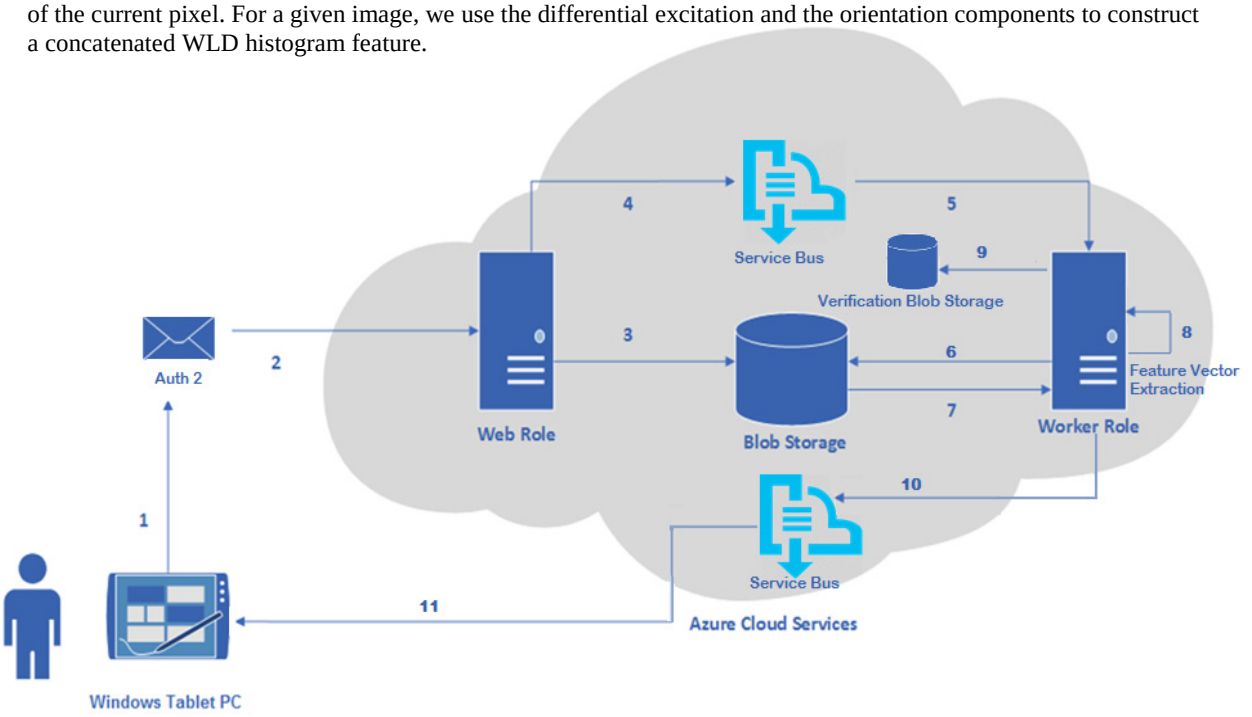

Figure 1.3 Verification Operation Architecture on Azure Cloud

- Classification

After all necessary features have been extracted, the final task is to decide whether or not a signature is forged or not, using the extracted features. There are obviously two decisions to make, this is essentially binary classification task. To learn the decision boundary between these two classes, the classifier is trained on the signature images. After that it takes help of what it learn to take a decision on the plotted images. Among the classifiers, the most popular classifiers which give better performance than the others is the K- nearest neighbourhood classifier.

7. Expected Results

- Capturing Biometric Traits and Authenticating user

The proposed online signature model on cloud platform addresses how the signatures will be acquired through the Windows tablet PC, by collecting and analysing the signature stroke information's such as X, Y coordinates and Pressure values. Thereafter, the user shall be authenticated using OAuth2 authentication framework

- Upload signature information into Azure

Signature information will be uploaded to the Azure cloud storage in blobs – as it will help in storing text and binary data, which will then help to process information on the cloud using the Web Roles and Worker Roles.

- Feature extraction using Webber Local Descriptor

Extract the various biometric traits of the retrieved signature from Azure storage, which shall be text data, using WLD feature extraction method.

- Classification using K-nearest Neighbourhood

The proposed model will make the online signature system highly learnable, by using classifiers. K-nearest neighbourhood is proposed to be used to enable the system to learn the various information which shall be retrieved through feature extraction.

- Performance Improvement

The proposed model is highly scalable, i.e., during unexpected traffic spikes, the web role and worker role can be automatically scaled up or down to meet demand, while simultaneously minimizing costs. The proposed online signature system gives 92.50 % PI (Performance Index) and 94.25% CCR (Correct Classification Rate).

This technology framework will provide a reliable environment for testing new releases without impacting the existing one, reducing the chances of unwelcomed customer downtime. The aim is to deploy the new release to production, by just swapping the staging environment into production. That will make the online signature system highly pluggable, it will also provide a much faster response time as compared to the traditional model. In this model the web role and worker role will be built on a high ended machine with a facility to scale up or scale down the configuration of this machines such as the CPU, RAM etc., with just a click of a buttons.

This research aims to replace the existing methodology of signature verification applications, which still uses traditional means to verify user signature by substituting it with a cloud based online signature framework, which can be easily used on any Windows compatible tablet PC – thus eventually transitioning such application verification process into 'BYOD' [Bring Your Own Device] category.

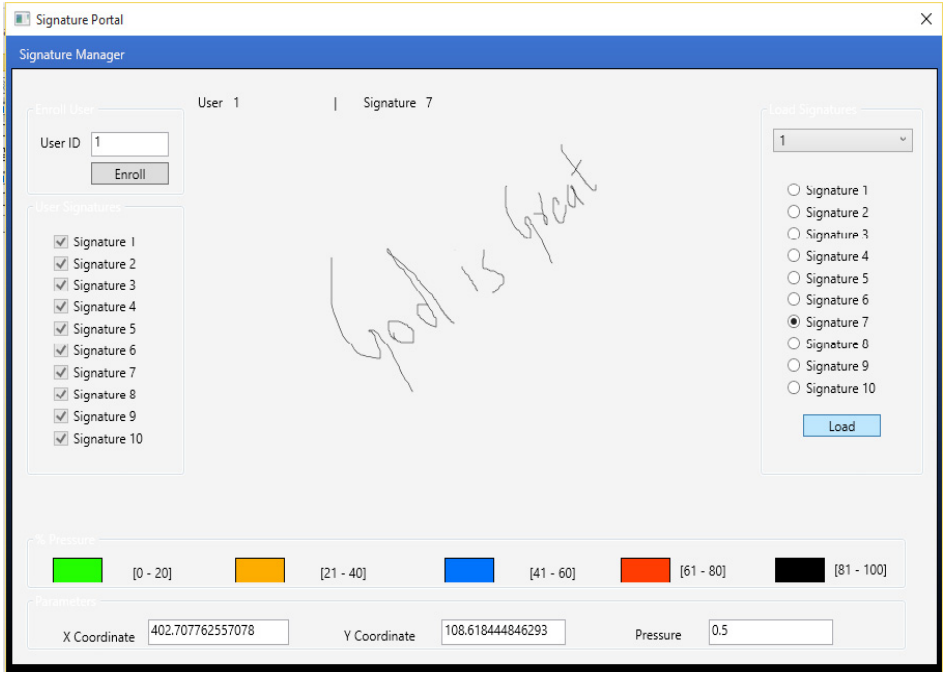

Figure 1.4 Tablet interface capturing user signatures: X, Y co-ordinates and Pressure information

References

1. Abdullah A. Albahdal and Terrance E. Boult: “Problems and Promises of Using the Cloud and Biometrics” Research Gate, Conference Paper · April 2014.
2. M. A. Sasse, S. Brostoff, and D. Weirich, Transforming the weakest links human/computer interaction approach to usable and effective security, BT technology, Journal, vol.19, no.3, pp.122–131, 2001.
3. Biometrics in the J. J. Yan, A. F. Blackwell, R. J. Anderson, and A. Grant, Password memorability and security: Empirical results, IEEE Security & privacy, vol. 2, no. 5, pp. 25–31, 2004
4. H B Kekre, V. A Bharadi, “Dynamic signature preprocessing by modified digital difference analyzer algorithm”, *Springer India, Thinkquest*, 978-81-8489-989-4_12, 2011
5. H B Kekre, V A Bharadi, T K Sarode , “Dynamic Signature Recognition using Time based Vector Quantization by Kekre’s Median Codebook Generation Algorithm”, *Springer India,Thinkquest*,10.1007/978-81-8489-989-4_46,2011
6. H B Kekre and V. A Bharadi, “Gabor Filter Based Feature Vector for Dynamic Signature Recognition”, *International Journal of Computer Applications* (0975 – 8887), vol 2 No: 03, May 2010.
7. H B Kekre and V. A Bharadi , “Texture Feature Extraction using Partitioned Complex Walsh Plane in Transform Domain for Iris and Palmprint recognition”, *in ICWET by IJCA journal* number-3, 2012.
8. A. S. Bommagani, M.C. Valenti, A. Ross, "A Framework for Secure Cloud empowered Mobile Biometrics", Proc. of IEEE Military Communications Conference (MILCOM), (Baltimore, MD), October 2014
9. Nilesh Y. Choudhary, Mrs. Rupal Patil, Dr. Umesh. Bhadade, Prof. Bhupendra M Chaudhari, “Signature Recognition & Verification System Using Back Propagation Neural Network”, *International Journal Of IT, Engineering And Applied Sciences Research (IJIEASR)* ISSN: 2319-4413 Volume 2, No. 1, January 2013.
10. Rupali Mehra, Dr.R.C.Gangwar, “Enhanced Offline Signature Recognition Using Neuro- Fuzzy and SURF Features Techniques”, *International Journal of Computer Science and Information Technologies*, Vol. 5 (5), 2014, ISSN: 0975-9646
11. Rafal Doroz, Malgorzata Palys, Tomasz Orczyk, Hossein Safaverdi, “Method Of Signature Recognition With The Use Of The Complex Features”, *Journal Of Medical Informatics & Technologies*, Vol. 23/2014, ISSN 1642-6037
12. D.G.Agrawal, Pranoti M. Jangale, Dynamic Texture Feature Extraction Using Weber Local Descriptor, *Int. Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 4,* March 2014
13. J. F. Vargas, M. A. Ferrer, C. M. Travieso, J. B. Alonso*: "*Off-line signature verification based on grey level information using texture features”, *Pattern Recognition, vol. 44, no.2, pp. 375-385,* 2011.
14. Pradeep Kumar* Shekhar Singh Ashwani Garg Nishant Prabhat, “Hand Written Signature Recognition & Verification Using Neural Network”, *International Journal Of Advanced Research In Computer Science And Software Engineering* Volume 3, Issue 3, March 2013, ISSN: 2277 128X
15. Darma Putra, Yogi Pratama, Oka Sudana and Adi Purnawan, “An Improved Dominant Point Feature for Online Signature Verification”, *International Journal of Security and Its Applications* Vol.8, No.1 (2014), ISSN: 1738-9976.